Exhibit A

Robert Tauler (SBN 241964)
rtauler@taulersmith.com
Wendy Miele (SBN 165551)
wmiele@taulersmith.com
Tauler Smith, LLP
626 Wilshire Boulevard, Suite 550
Los Angeles, California 90017
Tel: (310) 590-3927

Attorneys for Plaintiff
Anne Heiting

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

ANNE HEITING, an individual,

Plaintiff,

vs.

MARRIOTT INTERNATIONAL, INC., a Maryland Corporation; and DOES 1 through 25, inclusive,

Defendants.

Case No. 23STCV26803

COMPLAINT FOR:

1. **VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT (CAL. PENAL CODE § 631)**

2. **VIOLATIONS OF THE CALIFORNIA UNAUTHORIZED ACCESS TO COMPUTER DATA ACT (CAL. PENAL CODE § 502(e))**

JURISDICTION

1. Subject matter jurisdiction is proper in this Court because the amount in controversy is within this Court's jurisdictional limit.

2. This Court has personal jurisdiction over Defendant because, on information and belief, Defendant conducts a substantial amount of business in Los Angeles County, California.

3. Venue is proper in the Los Angeles County Superior Court pursuant to Code of Civil Procedure, §§ 394, 395, and 395.5. Wrongful conduct occurred and continues to occur in this County. Defendant conducted and continues to conduct business in this County as it relates to its illegal wiretapping. Additionally, Defendant has sufficient minimum contacts in the State of California or otherwise purposefully avails itself of the California market.

PARTIES

4. Plaintiff Anne Heiting ("Plaintiff") is a citizen of California residing within the Central District of California.

5. Defendant Marriott International, Inc. ("Defendant" or "Marriott") is a Massachusetts corporation that owns, operates, and/or controls marriott.com.

6. The above-named Defendant, along with its affiliates and agents, are collectively referred to as "Defendants." The true names and capacities of the Defendants sued herein as DOE DEFENDANTS 1 through 25, inclusive, are currently unknown to Plaintiff, who therefore sues such Defendants by fictitious names. Each of the Defendants designated herein as a DOE is legally responsible for the unlawful acts alleged herein. Plaintiff will seek leave of Court to amend the Complaint to reflect the true names and capacities of the DOE Defendants when such identities become known.

7. Plaintiff is informed and believes that at all relevant times, every Defendant was acting as an agent and/or employee of each of the other Defendants and was acting within the course and scope of said agency and/or employment with the full knowledge and consent of each of the other Defendants, and that each of the acts and/or omissions complained of herein was ratified by each of the other Defendants.

FACTUAL ALLEGATIONS

8. Marriott International, Inc. is the proprietor of marriott.com, an online platform provides consumers with booking options for hotels, vacations, meetings and events. During a browsing session on the Defendant's website, the plaintiff utilized the chat box feature. However, the plaintiff was not informed that her conversations were being recorded and exploited for commercial surveillance purposes without her consent. Defendant's deceptive and invasive practices violate the privacy rights of its customers.

9. In the context of Marriott's website, an iFrame (or Inline Frame) is a code that embeds content from another website ((in this case, SalesForce) within a web page. However, this code intercepts the inquiries that consumers believe are being sent directly to Marriott and diverts them to salesforce.com:

```
</div>
</div>
<script src="https://service.force.com/embeddedservice/menu/1678932281/channelMenu.min.js"></script>
<iframe id="eswframeForLog" src="https://d.la1-c1-ia7.salesforceliveagent.com/content/test/webdriver/logChannelMenu.html?parent=https://www.marriott.com/default.mi" style="display: none;"></iframe> == $0
<script type="text/javascript" src="https://marriottintl.secure.force.com/resource/1662529664000/SnapInSettings"></script>
<div id="auraErrorMessage"></div>
<!--render facet: 1:0-->
```

10. Once Salesforce gains access to the user's information, it stores it for its own purposes. Marriott fails to inform its website users that their communications are being monitored and stored using an "event listener" as seen below:

```
    }
    ;
    g.prototype.addCustomEventListener = function(a, c) {
        b.addMessageHandler("liveagent.customEventReceived", c);
        b.postMessage("chasitor.addCustomEventListener", a)
    }
    ;
    g.prototype.getSessionId = function() {
        return this.sid
```

11. Salesforce also shares the data it collects and stores with Marriott who adds the data to the existing profiles it has surreptitiously collected from its users. According to its own stated disclosures, Marriott collects a wide range of personal information from website users and consumers, including personal identifiers, device information, system data, browser information, operating system information, location details; such as GPS address and IP address, and may deduce additional demographic details like gender and age; various details about website usage; interactions with other websites, inferences and other information.

12. Visitors would be shocked and appalled to know that Defendant secretly records those conversations and pays third parties to eavesdrop on them in real time to be "targets" for non-descript mercantile campaigns. Defendant should not be permitted to acquire such extensive personal information from unsuspecting consumers who visit their website merely to make a purchase, such as booking a hotel room. This blatant disregard for consumer privacy is unacceptable and warrants appropriate scrutiny and intervention.

13. Within the past year, Plaintiff used the chat box feature on Marriott's site, however, Defendant did not inform Plaintiff that Defendant was not communicating with Marriott at all when chatting online on the marriott.com website. Marriott does not disclose its relationship at all to Salesforce or that Marriott is aiding, abetting, and paying third parties like Salesforce which is recording and commoditizing their communications using the seemingly harmless chat box feature. A feature which, because it is seemingly innocuous and appears to occur on Marriott's website, would never give rise to the suspicion that it is really a means to collect data and subvert privacy rights.

14. Defendant did not obtain Plaintiff's express or implied consent to wiretap or allow third parties to eavesdrop on visitor conversations, nor did Plaintiff know at the time of the conversations that Defendant was secretly wiretapping them and allowing third parties to eavesdrop on them.

FIRST CAUSE OF ACTION

Violations of the California Invasion of Privacy Act

Cal. Penal Code § 631(a)

15. Section 631(a) of California's Penal Code imposes liability upon any entity that "by means of any machine, instrument, contrivance, or in any other manner,"

(1) "intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system," or

(2) "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state" or (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section." Here, Defendant does all three.

16. Section 631 of the California Penal Code applies to internet communications and thus applies to Plaintiff's electronic communications with Defendant's Website. "Though written in terms of wiretapping, Section 631(a) applies to Internet communications. It makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.' Cal. Penal Code § 631(a)." *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022).

17. The software embedded on Defendant's Website to record and eavesdrop upon the Plaintiff's communications qualifies as a "machine, instrument, contrivance, or ... other manner" used to engage in the prohibited conduct alleged herein.

18. At all relevant times, Defendant aided, abetted, and even paid third parties to eavesdrop upon such conversations.

19. Plaintiff did not expressly or impliedly consent to any of Defendant's actions.

20. Defendant's conduct constitutes numerous independent and discreet violations of Cal. Penal Code § 631(a), entitling Plaintiff to injunctive relief and statutory damages.

SECOND CAUSE OF ACTION

Violations of the California Unauthorized Access to Computer Data Act

Cal. Penal Code § 502 (e)

21. The California Unauthorized Access to Computer Data Act ("CUCA") makes it unlawful for parties to obtain data from a computer user outside of the scope of their authorization.

22. Specifically, Penal Code Section 502(c) makes a party liable who "knowingly accesses and without permission"

(1) uses any computer data, in order to "wrongfully control or obtain" computer data, or

(2) "makes use of any data from a computer…" outside of the scope of authorization.

23. By collecting personal identifiers, device information, operating system information, characteristics such as age and gender; various details about website usage; inferences, and other information Defendant has exceeded the scope of its authorization from Plaintiff.

24. In fact, no authorization was provided by Plaintiff at all and no authorization for the data collection by means of using a chat box is ever requested or given.

25. Penal Code Section 502(c)(6) makes third parties liable if they "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section."

26. By allowing Salesforce to collect data from Plaintiff, including personal identifiers, website usage, and device information, and allowing it to use this information for its own purposes, Defendant has violated CUCA.

27. Section 502(e) provides a private right of action for "compensatory damages and injunctive relief or other equitable relief." Additionally, a court may award reasonable attorney's fees and punitive damages on a case-by-case basis.

PRAYER

WHEREFORE, Plaintiff prays for the following relief against Defendant:

1. An order declaring Defendant's conduct violates CIPA and CUCA;

2. An order of judgment in favor of Plaintiff against Defendant on the causes of action asserted herein;

3. An order enjoining Defendant's conduct as alleged herein and any other injunctive relief that the Court finds proper;

4. Statutory damages pursuant to CIPA and CUCA;

5. Punitive damages;

6. Prejudgment interest;

7. Reasonable attorneys' fees and costs; and

8. All other relief that would be just and proper as a matter of law or equity, as determined by the Court.

DATED: November 1, 2023

TAULER SMITH LLP

By: */s/ Robert Tauler*
Robert Tauler, Esq.
Attorney for Plaintiff
Anne Heiting

DEMAND FOR JURY TRIAL

Plaintiff Anne Heiting hereby demands a trial by jury.

DATED: November 1, 2023

TAULER SMITH LLP

By: */s/ Robert Tauler*
Robert Tauler, Esq.
Attorney for Plaintiff
Anne Heiting